

State of Transformation

Next Generation Risk Management for the Federal Government

ISACA Conference

April 20, 2010

Dr. Ron Ross

*Computer Security Division
Information Technology Laboratory*

Federal Government Transformation

The emerging information security publications support government-wide transformation for risk management and driven by...

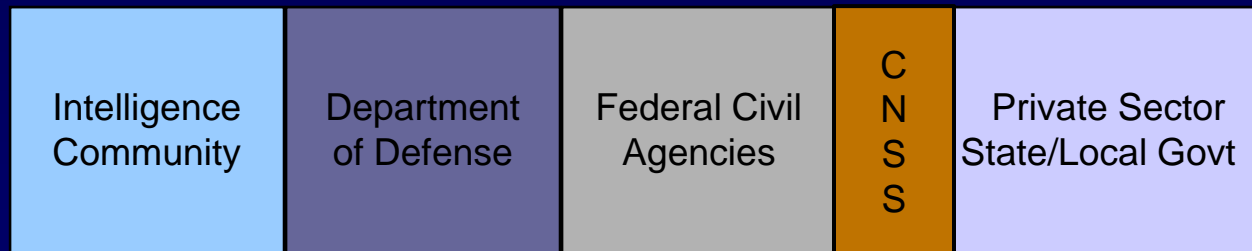
- Increasing sophistication and operations tempo of cyber attacks.
- Convergence of national and non-national security interests within the federal government.
- Convergence of national security and economic security interests across the Nation.
- Need for a unified framework in providing effective risk-based cyber defenses for the federal government and the Nation.

Unified Information Security Framework

The Generalized Model

**Unique
Information
Security
Requirements**

The “Delta”



**Common
Information
Security
Requirements**

Foundational Set of Information Security Standards and Guidance

- Risk management (organization, mission, information system)
- Security categorization (information criticality/sensitivity)
- Security controls (safeguards and countermeasures)
- Security assessment procedures
- Security authorization process


National security and non national security information systems

What We Have Accomplished...

Joint Task Force Transformation Initiative

Core Risk Management Publications

- NIST Special Publication 800-53, Revision 3
Recommended Security Controls for Federal Information Systems and Organizations

Completed
- NIST Special Publication 800-37, Revision 1
Applying the Risk Management Framework to Federal Information Systems: A Security Lifecycle Approach

Completed
- NIST Special Publication 800-53A, Revision 1
Guide for Assessing the Security Controls in Federal Information Systems and Organizations
Projected June 2010

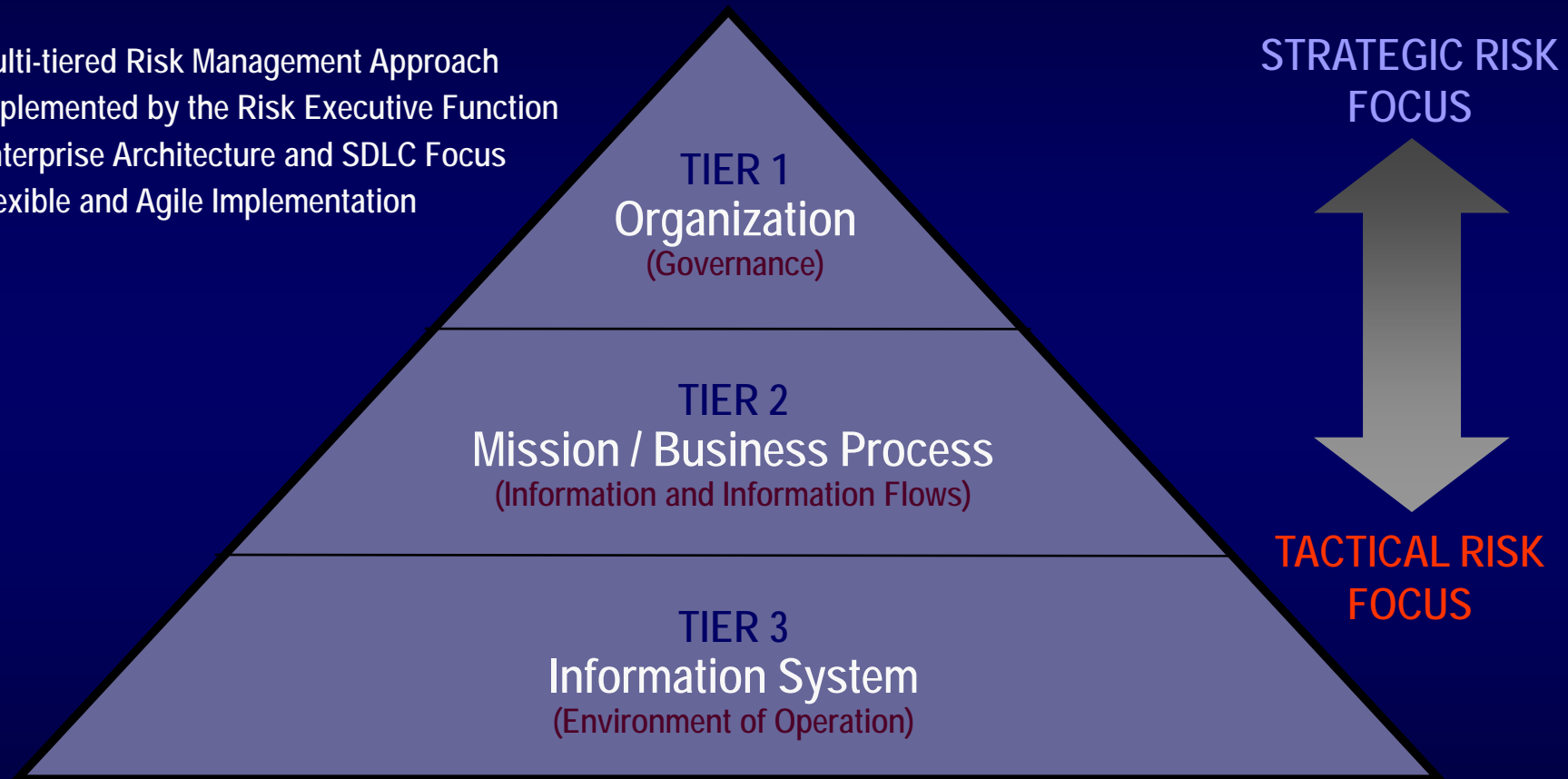
Joint Task Force Transformation Initiative

Core Risk Management Publications

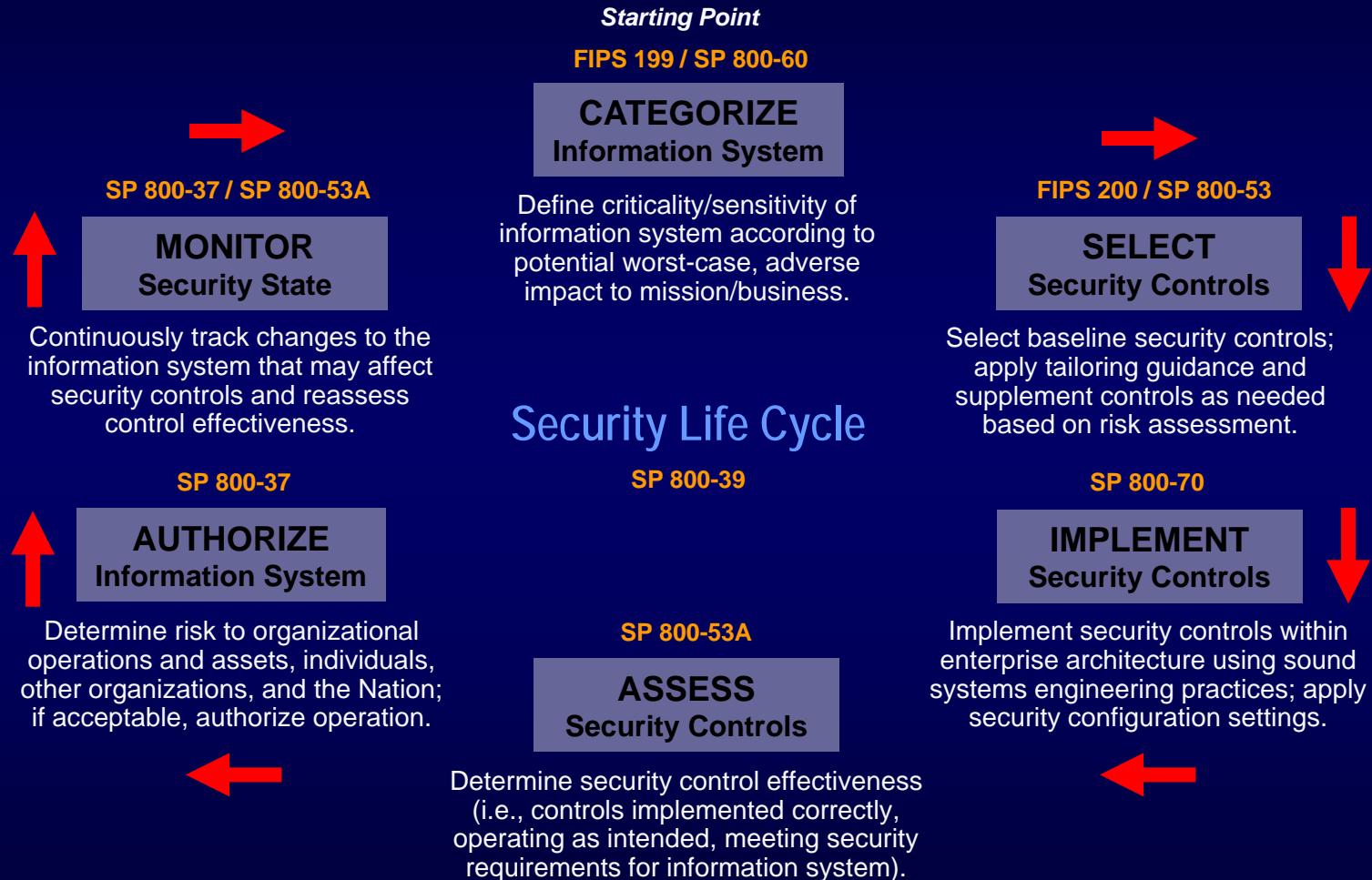
- NIST Special Publication 800-39
Enterprise-Wide Risk Management: Organization, Mission, and Information Systems View
Projected November 2010
- NIST Special Publication 800-30, Revision 1
Guide for Conducting Risk Assessments
Projected November 2010

Enterprise-Wide Risk Management

- Multi-tiered Risk Management Approach
- Implemented by the Risk Executive Function
- Enterprise Architecture and SDLC Focus
- Flexible and Agile Implementation



Risk Management Framework



Characteristics of Risk-Based Processes

(1 of 3)

- Integrates information security more closely into the enterprise architecture and system development life cycle.
- Provides equal emphasis on the security control selection, implementation, assessment, and monitoring, and the authorization of information systems.
- Promotes near real-time risk management and ongoing system authorization through the implementation of robust continuous monitoring processes.

Characteristics of Risk-Based Processes

(2 of 3)

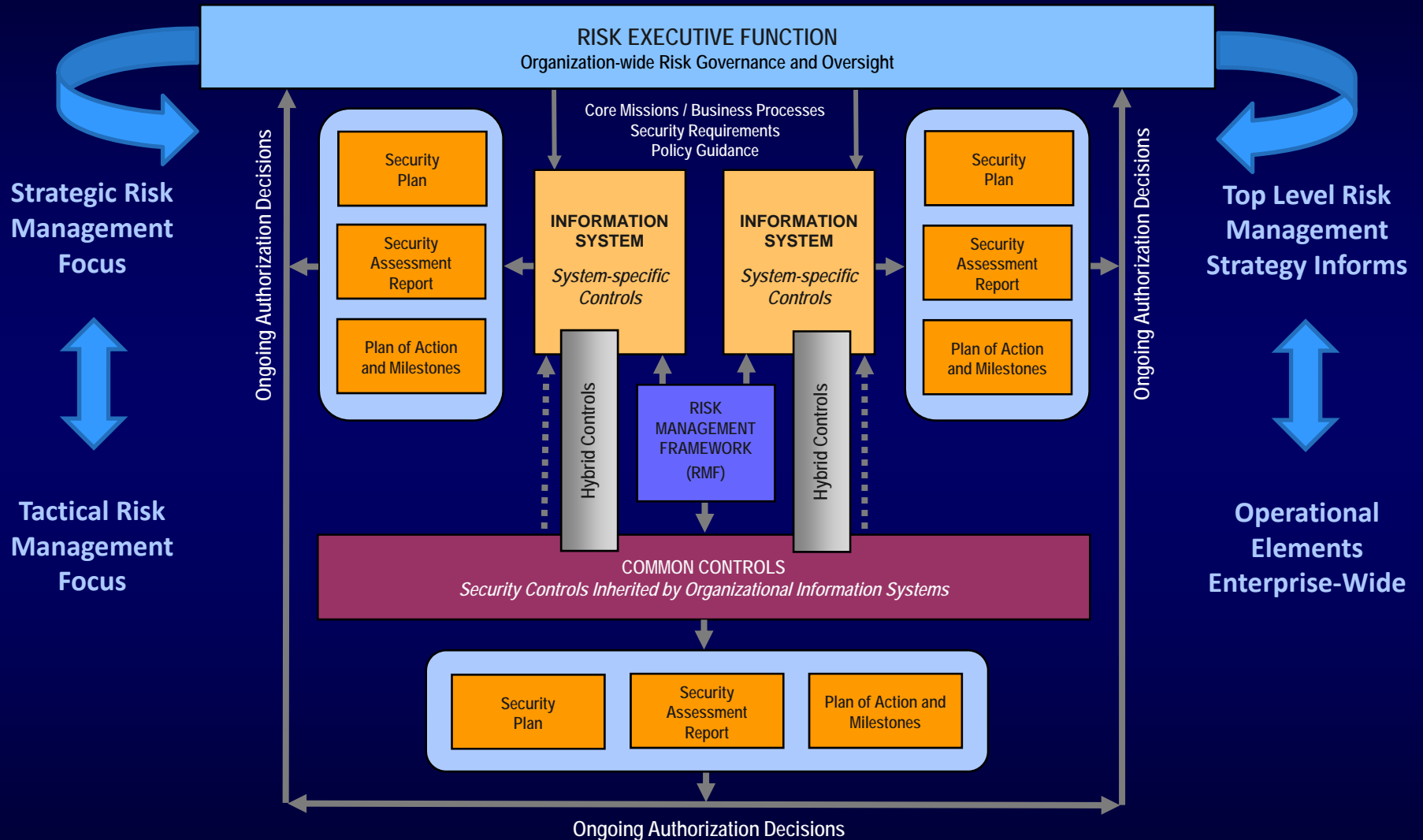
- Links risk management activities at the organization, mission, and information system levels through a risk executive (function).
- Establishes responsibility and accountability for security controls deployed within organizational information systems and inherited by those systems.
- Encourages the use of automation to increase consistency, effectiveness, and timeliness of security control implementation.

Characteristics of Risk-Based Processes

(3 of 3)

- Provides senior leaders the necessary information to make credible, risk-based decisions with regard to the information systems supporting their core missions and business functions.

Managing Complex Risk Activities



Expanded Authorization Approaches

- Traditional Authorization
(single authorization official)
- Joint Authorization
(multiple authorization officials)
- Leveraged Authorization
(reuse of authorization results)

Looking to the future...

2010 Focus Areas and Initiatives

- Common Security Standards and Guidance
 - Joint Task Force Transformation Initiative (DoD, IC, NIST, CNSS)
 - Unified Information Security Framework
 - Core risk management and information security publications
 - Additional publications for partnership collaboration
 - Privacy Appendix for SP 800-53, Revision 3 (privacy controls)
 - Threat Appendix for SP 800-53, Revision 3 (Cyber Prep Initiative)
- Developmental Security
 - Systems and Security Engineering Guideline
 - Application Security Guideline

2010 Focus Areas and Initiatives

- Operational Security
 - S-CAP Initiative and future extensions (network devices, mainframes)
 - Continuous Monitoring Guideline
 - Configuration Management and Control Guideline
- Education, Training, and Awareness
 - FISMA Phase II Training Modules
 - Automated support tools
 - Outreach program to State and local governments; private sector
- Prototypes and Use Cases
 - Industrial Control Systems

Public and Private Sector Partnerships

- Over 90% of critical infrastructure systems/applications owned and operated by non federal entities.
- Key sectors:
 - Energy (electrical, nuclear, gas and oil, dams)
 - Transportation (air, road, rail, port, waterways)
 - Public Health Systems / Emergency Services
 - Information and Telecommunications
 - Defense Industry
 - Banking and Finance
 - Postal and Shipping
 - Agriculture / Food / Water / Chemical



Contact Information

100 Bureau Drive Mailstop 8930
Gaithersburg, MD USA 20899-8930

Project Leader

Dr. Ron Ross
(301) 975-5390
ron.ross@nist.gov

Administrative Support

Peggy Himes
(301) 975-2489
peggy.himes@nist.gov

Senior Information Security Researchers and Technical Support

Marianne Swanson
(301) 975-3293
marianne.swanson@nist.gov

Kelley Dempsey
(301) 975-2827
kelley.dempsey@nist.gov

Pat Toth
(301) 975-5140
patricia.toth@nist.gov

Arnold Johnson
(301) 975-3247
arnold.johnson@nist.gov

Web: csrc.nist.gov/sec-cert

Comments: sec-cert@nist.gov